

(11)Publication number : 2003-051818
(43)Date of publication of application : 21.02.2003

(72)Inventor : YOKOTE AKI

Priority number : 2001 827632 Priority date : 06.04.2001 Priority country : US

<http://www19.ipdl.ncipi.go.jp/PA1/result/detail/main/wAAAJEaqVTDA415051818...> 2006/05/01

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

【特許請求の範囲】

【請求項 1】 移動 IP ネットワークにおいてインターネットプロトコルセキュリティを実行する方法であつて、

第一ノードからの第二ノードに対する通信を初期化する過程と、

前記第一ノードが、前記第二ノードにおいてセキュリティアソシエーションが設定されているかどうかを判断する過程と、

前記第一ノードが、前記第二ノードにおいてセキュリティアソシエーションが設定されていない場合は、前記第二ノードと行う通信を保護するためのセキュリティアソシエーションの設定を初期化する過程とを有することを特徴とするインターネットプロトコルセキュリティ実行方法。

【請求項 2】 前記第二ノードは、自身のホームリンクの外部に位置する移動ノードであることを特徴とする請求項 1 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 3】 前記第一ノードは、前記第二ノードのホームエージェントを介して前記第二ノードへ制御パケットを送信することによって前記第二ノードとの通信を初期化し、前記第二ノードはそれに対する応答として、バインディング更新を前記第一ノードへ送信することを特徴とする請求項 2 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 4】 前記設定されるセキュリティアソシエーションには、ケルベロス鍵交換法が用いられることを特徴とする請求項 1 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 5】 前記第一ノードおよび前記第二ノードの少なくとも 1 つは、第二層で設定される秘密鍵を第三層での認証に用いることを特徴とする請求項 4 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 6】 前記ネットワークはセキュリティアソシエーション管理装置を有し、前記セキュリティアソシエーションは前記セキュリティアソシエーション管理装置によって設定されることを特徴とする請求項 1 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 7】 前記第一ノードおよび前記第二ノードは加入者識別モジュールを有し、前記設定されるセキュリティアソシエーションは前記加入者識別モジュールに格納されることを特徴とする請求項 1 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 8】 前記セキュリティアソシエーションの有効期間は長く、前記第一ノードと前記第二ノードの間で行われる複数の通信セッションに渡って用いられることを特徴とする請求項 1 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 9】 前記通信はリアルタイム双方向デジタル

データ通信であることを特徴とする請求項 1 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 10】 前記リアルタイム双方向デジタルデータ通信はインターネットプロトコルを用いた音声通信であることを特徴とする請求項 9 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 11】 前記ネットワークは、国際移動通信規格 2000 に適合したものであることを特徴とする請求項 1 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 12】 移動 IP ネットワークにおいて、ケルベロスを用いたインターネットセキュリティプロトコルを実行する方法であつて、

ノードが無線基地局と無線による接続をしているときに、前記ノードと前期無線基地局との間で第二層の秘密鍵を設定する過程と、

前記設定された第二層の秘密鍵を前記ノード内において第二層から第三層へ通知する過程と、

前記ノードが前記ネットワークにログインするときに、前記ノードを前記ネットワークに認証させるために、前記通知された第二層の秘密鍵を用いる過程とを有することを特徴とするインターネットプロトコルセキュリティ実行方法。

【請求項 13】 前記ノードが行う通信はリアルタイム双方向デジタルデータ通信であることを特徴とする請求項 12 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 14】 前記リアルタイムデジタルデータ通信はインターネットプロトコルを用いた音声通信であることを特徴とする請求項 13 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 15】 前記ネットワークは国際移動通信規格 2000 に適合したものであることを特徴とする請求項 12 に記載のインターネットプロトコルセキュリティ実行方法。

【請求項 16】 複数のノードがお互いにネットワークを介して通信を行い、

前記複数のノードのセキュリティアソシエーションを管理するための複数のセキュリティアソシエーション管理装置が前記ネットワーク上に設けられ、第二ノードとの通信を行う必要のある第一ノードから要求を受けると、一のセキュリティアソシエーション管理装置は、以前に前記第二ノードと行った通信の際に設定されたセキュリティアソシエーションが当該セキュリティアソシエーション管理装置内に格納されている場合は、当該セキュリティアソシエーションを前記第一ノードへ送信し、以前に前記第二ノードと行った通信の際に設定されたセキュリティアソシエーションが格納されていない場合は、当該セキュリティアソシエーション管理装置は当該セキュリティアソシエーションの設定を行い、設定されたセキ

セキュリティアソシエーションを当該セキュリティアソシエーション管理装置内へ格納し、前記第一ノードへ送信することを特徴とするIPネットワーク。

【請求項17】 前記ネットワークはケルベロス鍵交換法を採用し、通信を行う必要があるノードに対応したセキュリティアソシエーション管理装置に対し、セッション鍵を配布する鍵配布センタを備えることを特徴とする請求項16記載のIPネットワーク。

【請求項18】 前記セキュリティアソシエーション管理装置は、前記鍵配布センタに対しセッション鍵の発行を要求することを特徴とする請求項17記載のIPネットワーク。

【請求項19】 前記通信はリアルタイム双方向デジタルデータ通信であることを特徴とする請求項16記載のIPネットワーク。

【請求項20】 前記リアルタイム双方向デジタルデータ通信はインターネットプロトコルを用いた音声通信であることを特徴とする請求項19記載のIPネットワーク。

【請求項21】 前記ネットワークは国際移動通信規格2000に適合するものであることを特徴とする請求項16記載のIPネットワーク。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は広く無線通信ネットワーク及びモバイルインターネットプロトコルベースのネットワークにおいて導入されるインターネットプロトコルセキュリティ(IPsec)、特に「Voice over IP」(VoIP)のような第三世代およびそれ以上の世代のリアルタイム・インタラクティブ・デジタルデータ通信、移動通信、インターネットプロトコルベースのデータ通信ネットワーク、または無線LANに適用されるIPsecに関する。

【0002】

【従来の技術】デジタルデータ通信ネットワークは、アメリカをはじめ、世界中で、ビジネス、商取引、あるいは一般の人々の生活においていたるところに顔を見せるようになった。公益的性格の強いインターネット、私的なプライベートローカルネットワーク(LAN)、広域エリアネットワーク(WAN)は、ますますデータ通信、データ送受信の重要なバックボーンとなっている。電子メール、ファイルアクセス、ファイル共有、サービスアクセスおよびサービス共有は、そのような多くのネットワークによって供給されるデータ通信サービスやデータ通信アプリケーションのうちのほんの一部でしかない。

【0003】インターネットを含む今日のほとんどのデータ通信ネットワークは、実質的に同じアドレス管理プロトコルとルーティングプロトコルに従っている。このプロトコルにおいては、各々のネットワークにアクセス

することのできる装置(ノード)やネットワーク上に設けられたサーバ(ルータ)は、IPアドレスと呼ばれるただ一つのアドレスを持っている。ネットワーク内またはネットワーク間でデジタルデータをやり取りするためには、送信者(送信ノード)はデータを「パケット」に分割して送信する。各々のパケットは送信ノードや所望の送信先ノードのIPアドレスやその他の情報のような、プロトコルによって定められている通信コントロールデータ、、、及び送信先ノードに送るべき実質的なデータを含んでいる。一回のデータの通信には、通信されるデータ量とその他の要素とに応じた数のパケットが作られ送信される。送信ノードは各々のパケットを別途独立に送信する。パケットはネットワーク上の中間ルータによって送信ノードから送信先ノードへと送られる。それら複数のパケットはかならずしも同じ経路をへて送信先ノードへ送られる必要はないし、また同時に到着する必要もない。なぜならパケット化の過程において各々のパケットには連続的な標識が付けられるからである。この標識によって送信先ノードは、たとえ異なった順番、異なる時間にパケットが届いたとしても、パケットを元の順番通りに再構成することができ、従ってパケットからもとのデータを再構築することができるのである。

【0004】データ通信ネットワークの世界標準規格策定における認定機関であるインターネット学会の通信通信連合(ITU)は、最近、国際移動通信規格(IMT-2000)を制定した。この規格は携帯電話、PDA(Personal Digital Assistants)、ハンドヘルドコンピュータ等の無線によって通信を行う広範囲な移動アクセスを考慮に入れた、いわゆる第三世代(3G)およびそれを超える世代(すなわち3.5G、4G等)のデータ通信ネットワークを提案している(<http://www.itu.int>参照)。

【0005】そのなかで提案されている第三世代およびそれをこえる世代の通信ネットワークは、データ通信に基づくIPをサポートしている。すなわち、すべてのネットワーク上のデータはデジタルデータであり、パケット単位で、そしてインターネットで用いられるアドレス管理プロトコル及びルーティングプロトコルに従ってやり取りされる。さらに、上述した第三世代及びそれ以上の世代無線通信ネットワークにおいては、移動ノードは、ネットワークに接続された他の固定ノードまたは移動ノードとデータ通信を行っている間、ネットワーク内を自由に移動することができる。従って、移動ノードがネットワーク接続やパケットの伝達経路を変更した場合、そのようなネットワークは、セキュリティや認証に関する問題を処理するとともに、移動ノードのアドレス管理装置、通信ノード間でやり取りされるデータパケットのダイナミックルーティングを提供しなくてはならな

【0006】近い将来、インターネットを使用するノードのうち大部分或いは少なくともかなりの部分を移動ノードが占めると予想されるので、この移動ノードに適した通信ネットワークを構築することが特に重要となっている。インターネットアーキテクチャおよびインターネットの効率的利用に関するネットワークの設計者、運用者、ネットワーク機器の販売業者、学術研究者の国際的共同体であるインターネット技術特別対策委員会(IETF)は、モビリティ支援に関するいくつかの規格を提案している(<http://www.ietf.org> 参照)。これらの提案には、IETFのRFC2002(モバイルIPバージョン4(IPv4)とも呼ばれる)や「IPv6におけるモバイル支援(Mobility Support in IPv6)」と表された草案「draft-ietf-mobileip-ipv6-13」(モバイルIPバージョン6とも呼ばれる)といったモビリティ支援に関する規格が含まれている。この2つの規格は本願明細書において参照として援用される。

【0007】IPv4やIPv6で定義されるプロトコル運用によると、移動ノードはその移動ノードのIPアドレスを変更せずにあるリンクから別のリンクへと移動することができる。ホームリンク上のホーム・サブネット・プレフィックス内で移動ノードに割り当てられた1つのIPアドレスである「ホームアドレス」によって移動ノードの位置は常に把握される。パケットはこのアドレスを用いて、移動ノードの現在の地点からインターネットにアクセスしているかに関係なく転送され、移動体が別のリンクに移動しても、移動ノードは相手先ノード(固定ノード、移動ノードを含む)と通信を行い続けることができる。それゆえ、移動ノードがホームリンクから移動しても、トランスポート層と上位レイヤのプロトコルやアプリケーションに影響を与えない。

【0008】モバイルIPv6はモバイルIPv4と多くの点で共通するが、プロトコルに関して言えば、完全にIPを包含しつつモバイルIPv4よりも多くの改良がなされている。例えば、「経路最適化」はモバイルIPv6のプロトコルの基本的な部分であるが、これはモバイルIPv4においては付加的な拡張オプションでしかなく、全てのノードでサポートされることは想定されていない。

【0009】経路最適化機能によって移動ノードと相手先ノードとの間で直接的な経路が設定され、パケットの転送効率は最適化される。上述したように、それぞれの移動ノードは、現在のインターネットへの接続ポイントにかかわらず、常にホームアドレスによって識別される。移動ノードがホームリンクから離れている場合には、移動ノードは気付けアドレスとも関連付けられており、そこには現在インターネットに接続している当該移動ノードの位置に関する情報が含まれている。

【0010】モバイルIPv4においては、ホームから

離れている使用されている移動ノードはホームエージェントに気付けアドレスを登録する。同様にモバイルIPv6においても、ホームリンクの外部に位置している移動ノードは、登録要求をホームエージェントに送信することによってホームエージェントに気付けアドレスを告知する。ホームエージェントは、登録要求を受信した後、当該移動ノード宛のパケットを取得すると、当該移動ノードの気付けアドレスへトンネリングによって転送する。

10 【0011】しかしながら逆方向の通信では、パケットは移動ノードから直接相手先ノードへ送られる。よって、いわゆるパケットのトライアングル・ルーティングが発生し、非対称パケット遅延の問題が生じてしまう。相手先ノードから移動ノードへの直接転送経路を確立するため、相手先ノードには、当該移動ノード現在の気付けアドレスを通知されるからである。モバイルIPv4においては、ホームエージェントが相手先ノードからホームから離れている移動ノード宛のパケットを受信したとき、バインディング情報をIPv4の移動ノードに送信することによって、直接転送経路が確立される。モバイルIPv6では、モバイルノードがバインディング更新を直接相手先ノードに対して送信することによって直接転送経路の確立がなされる。

【0012】モバイルIPにおいてはセキュリティに関する問題も存在する。例えば、モバイルIPv4における位置登録プロトコルにおいては、移動ノードの通信は気付けアドレスにトンネリング転送されるホームエージェントとモバイルエージェントとの間で位置登録が認証されない場合、このトンネリング転送によって通信ネットワークは非常に脆弱なものになってしまう可能性がある。さらに、モバイルIPv6においてバインディング更新は直接移動ノードへ転送されるのが標準となっている。従って、移動ノードと相手先ノードとの間でバインディング情報を含むパケットが認証されなかった場合、パケットの経路が変更されるとセキュリティ上の問題が生ずる可能性がある。モバイルIPを導入することによるこのようなセキュリティ上の問題は以前から指摘されていた。

40 【0013】実際、関連RFC提案においてそのようなセキュリティ上の問題が取り上げられているが、それらはモバイル環境においてIPセキュリティ(IPsec)導入の必要性を指摘するにとどまり、その具体的な導入方法には一切触れていない。IETFのモバイルIP審議会においてはモバイル環境に適用可能なIPsecの構想に関して議論・研究されているにもかかわらずである。

【0014】一方、IPsecの構成の基礎はIETFのRFC2401に「インターネットプロトコルのセキュリティ構成(Security Architecture for the Internet Protocol)」と称して規定されており、本願明細書

において参考として援用される。RFC 2401には、例えば接続の安定性、データ元の認証、秘匿性等の問題を扱うためのセキュリティサービスを含む、暗号を用いたIPsecが提案されている。基本的には、RFC 2401で提案されているIPsecは共通暗号鍵のみに依存しており、送信者と受信者の間の通信はその鍵によって暗号化、復号化される。したがって、RFC 2401で提案されるIPsecが機能するためには、送信者と受信者との間で安全な通信が行われる前に、暗号鍵と認証アルゴリズムまたは暗号化アルゴリズムと、そのアルゴリズムを実行するのに必要なパラメータとに関して両者の間で合意が成立している必要がある。この合意はセキュリティアソシエーション(SA)と呼ばれている。暗号鍵を設定する一般的な方法は鍵の配送・生成である。鍵の配送の例としては、第三者の認証機関から供給された共通暗号鍵を利用する方法がある。鍵の生成方法で最も利用されているものの一つとして、ディフィ・ヘルマン(Diffie-Hellman; D-H)アルゴリズムがある。

【0015】D-Hアルゴリズムは、送信者と受信者の各々は自分の持つ秘密の情報と相手の持つ公開情報とを数学的に結合させ共有の暗号値を計算する方法である。鍵管理プロトコルの詳細についてはRFCの「インターネット・セキュリティ委員会および鍵管理プロトコル(Internet Security Association and Key Management Protocol)」を参考のため本願明細書において援用することとする。

【0016】上述したIPsecはモバイルIPv4環境およびモバイルIPv6環境の両方に適用可能である。例えば、モバイルIPv4における、ホームから離れている移動ノードが気付けアドレスをホームエージェントに登録している間、当該ホームエージェントと当該移動ノードは互いに合意できるSAについて協議し、その後のトンネルを介した通信を保護するために用いられる暗号鍵を設定する。同様に、上記IPsecはモバイルIPv6における経路最適化過程において実行される。すなわち、ホームから離れている移動ノードはバインディング更新を相手先ノードへ送信することによって、当該移動ノードの現在のインターネットへの接続ポイントを通知する。次に移動ノードと相手先ノードは互いに合意できるSAを協議し、その後の直接経路で行われる通信を保護するために使用すべき暗号鍵を決定する。

【0017】上述した提案されているIPsec構成は、比較的モバイルIP環境でよく機能する。また、このIPsecの改良および効果的な実行に努力が払われている。しかし、以下の問題が考えられる。例えば、モバイル環境において提案されているIPsecは、経路最適化がなされたときに移動ノードと相手先ノードとの間でSAを設定する過程において一定の時間が必要とな

る。IPsecの本来の目的からすると、保護すべき通信はSAが確立される前に行われてはならない。従って、SAの確立のためには時間が必要であり、これは明らかに通信の遅延を招く。通信の遅延は、電子メールやファイルの送受信に関しては深刻な問題を引き起こさないかもしれない。そのようなデータ通信はリアルタイムの双方向アプリケーションでなく、したがって特に通信の遅延には影響されないからである。

【0018】

10 【発明が解決しようとする課題】しかしながら、近年のVoIPやリアルタイム双方向マルチメディアのようなリアルタイム双方向データ通信の登場により、モバイル環境においてIPsecを導入することはかなり困難になってしまっている。電子メールやファイルの送受信と違い、リアルタイムデータ通信アプリケーションはタイミングのずれに非常に敏感である。特にVoIPはインターネットワーク処理、送受信、ルーティング遅延に非常に敏感である。SAの確立に要する時間に起因した通信の遅延は、鍵を設定する際にD-Hアルゴリズムのような大量の計算を必要とする鍵生成方法が用いられた場合に、より顕著となる。

【0019】

【課題を解決するための手段】本発明の目的は必要な認証およびセキュリティアソシエーション設定過程で生ずるパケット遅延を減少させる方法を提供することである。具体的には、本発明は、受信ノードがパケットを送信ノードから受信した後その過程を初期化するのを待つのではなく、当該送信ノードがユーザ認証およびセキュリティアソシエーションの設定を初期化することができる方法を提供する。

【0020】本発明の方法によれば、送信ノードは受信ノードとの間の通信を初期化し、当該受信ノードに対してセキュリティアソシエーションが設定されたかどうかを判定する。当該セキュリティアソシエーションが設定されていない場合、送信ノードはセキュリティアソシエーションの設定を初期化する。受信ノードが自分のホームリンクの外部にいることもあるが、この場合には当該受信ノードは送信ノードからパケットを受信した後バインディング更新を送信する。本発明においては、送信ノードがバインディング情報を受信ノードから受信する前にセキュリティアソシエーションの設定が初期化される。従って、本発明の方法をもちいることによって、認証とセキュリティアソシエーションの設定の過程において発生するパケット遅延が減少する。

【0021】本発明の一態様においては、認証およびセキュリティ確保の過程においてケルベロス鍵交換方法が用いられる。ケルベロス鍵交換方法は計算量が少なく済むので、PDAや携帯電話等のあまりリソース利用ができない機器が主に利用する通信ネットワークであるモバイルIP通信ネットワークに適している。計算量が少

ないため認証およびセキュリティアソシエーションの確立に要する時間は少なくて済む。よって、認証及びセキュリティアソシエーションに起因するパケット遅延はさらに減少する。

【0022】本発明の別の態様において、モバイルノードの無線通信ネットワーク制御装置(RNC)に対するレイヤ2の秘密鍵は、レイヤ3の事前共有秘密鍵としても用いられ、当該移動ノードが当該通信ネットワークにアクセスする際の認証がなされる。これによって、移動ノードにおいて鍵の管理作業が用意になる。

【0023】本発明のさらに別の態様において、通信ネットワークは当該通信ネットワークに接続されるノードのSAを管理するSA管理装置を備えている。SA管理装置を設けることによって、PDAや携帯電話等のリソースの少ないノードの消費メモリ量およびノードが行うべき計算量が軽減される。携帯電話の消費メモリ量は、加入者識別モジュール(SIM)にSAを格納しておくことによって削減可能である。

【0024】

【発明の実施の形態】本発明の好適な実施形態を図面を参照しつつ説明する。この図面において、同様の構成要素には同一の参照符号が付される。本願明細書における好適な実施形態の説明は本質的な意味において例示に過ぎず、本発明の範囲を限定するものではない。

【0025】図1に本発明が適用される第三世代の無線モバイルアクセスIPネットワーク100の一例を示す。データ通信ネットワーク100は、モバイルアクセス通信ネットワークに対するIMT-2000規格およびITUの仕様に従うものとする。加えて、データ通信ネットワーク100は、IETFで提案されているモバイルIPv6およびモバイルIPv4標準規格に従い、モバイルIP支援を実行する。これらの規格および仕様はITUおよびIETFのウェブサイトで公開されており、本願明細書において参照として援用される。

【0026】無線モバイルアクセスIP通信ネットワーク100の中心には、多数の図示せぬノードつまり固定の接続ポイントまたはリンクを有する固定ノードIPデータ通信ネットワーク120が設けられている。インターネットプロトコルバージョン6などのインターネットプロトコルに従って、デジタルデータは通信ネットワーク内または通信ネットワークを介してやり取りされる。インターネットプロトコルバージョン6はIETFのRFC2460に規定されており、これを本願明細書において参照として援用することとする。基幹通信ネットワーク120には複数の関門ルータ130が設けられており、これらが集まってIPモバイルバックボーン140を形成している。データパケットは、従来のインターネットアドレス管理およびルーティングプロトコルに従い、ネットワークに接続された送信元から送り先ノードへと転送される。おのおのの関門ルータ130は一つの

IPアドレスを持ち、ホームエージェント(HA)またはフォーリンエージェント(FA)として機能するサーバ又はルータ145と接続されており、移動ノード135および相手先ノード140とコア・ネットワーク120とを接続している。これはIETFのRFC2002(「Mobile IP Version4」)で規定されているもので、これは本願明細書において参照として援用される。移動ノードと及び相手先ノードは異なる種類の携帯受話器、携帯電話機、ハンドヘルドコンピュータ、PDA(Personal Digital Assistants)、無線データ通信端末等のモバイル無線通信デバイスであってもよい。

【0027】RFC2002に従うと、移動ノード135及び相手先ノード140は一つのホームネットワークが与えられる。各ノード135,140は、そのホームネットワーク上での実質的なルータであるホームエージェント145をさらに有する。おのおのの移動ノード130および相手先ノード145が自身のホームネットワーク内に位置しているときは、そのホームエージェントが通信ネットワーク120への接続ポイントとなる。すなわち、移動ノードがホームネットワーク内にいる場合は、当該移動ノードのホームエージェント145は移動ノードからのパケットを転送する。

【0028】また、提案されているモバイルIP支援の規格に従うと、モバイルノードのホームエージェント145は、移動ノード135の現在位置に関する情報、すなわち当該移動ノードの気付けアドレスを保持し、移動ノード135がそのホームネットワークエリアから離れて作動しているとき、少なくとも提案されている基本的なモバイルIPv4規格では、パケットの転送およびトンネリング送信をホームネットワークエリアの外部に位置している当該移動ノード135に対して行い続ける。

【0029】他のルータ145はフォーリンエージェントとして機能する。フォーリンエージェントは、移動ノードがホームネットワークエリアの外部で動作するときは、当該移動ノード135に対しアクセスポイントを提供する。移動ノードが、ある時間および位置において接続している通信ネットワークに属するフォーリンエージェントは、当該移動ノード135から、また当該移動ノード135へとパケットを転送する機能を有する。各エージェント145は無線基地局通信ネットワーク150を有しており、モバイルノード135および140と通信を行うようになっている。各無線基地局通信ネットワーク150は複数の無線基地局(BTS)を有している。移動ノード135および140、BTSはCDMA、W-CDMAまたは同様なデジタルデータ通信技術を用いて、相互に通信を行う。BTS通信ネットワーク150および155の構成、配置および機能は従来の一般的なものである。同様に、無線移動ノード135およびBTS155にはCDMA、W-CDMAや同様のデ

デジタルデータ通信技術が標準的に用いられる。その詳細な説明は、本発明の理解には必要でない故省略する。

【0030】各ノードは開放型システム間相互接続（OSI）規格に準拠しパケットの送受信を行う。OSI規格は7つの離散的レイヤ、すなわちアプリケーション層（第7層）、プレゼンテーション層（第6層）、セッション層（第5層）、トランスポート層（第4層）、ネットワーク層（第3層）、データリンク層（MAC）（第2層）、および物理層（第1層）における通信プロトコルの実行の枠組みを定義している。OSI規格によれば、送信ノードの第7層から始まり、制御は一つの層から次の層へ渡されてゆき、第一層まで下っていく。そして通信ネットワークを介して、相手先ノードにおいて、制御が最下層から最上位層まで上っていく。最下層では基本的な通信プロトコルの制御が行われる。例えば、第一層はBTSへビットデータを送信したり、BTSから受信したりする。この層はビットのもつ意味を解釈しないが、信号の電気的特性および物理的な特性あるいは信号方式を取り扱う。第2層はBTSとの通信における伝送データのビット誤りおよびビット列フォーマットを担当する。すなわちこの層はビットの意味をある程度解釈し、BTSとの間の通信プロトコルを取り扱う。第3層はネットワーク上の通信経路の確立を担当する。この層は、データの意味を完全に解釈しアドレス管理（アドレッシング）、ルーティングおよびセキュリティプロトコルの処理を行う。

【0031】データ通信ネットワーク100全体において、移動ノードモビリティには3つの段階がある。第一に、マクロモビリティとは、移動ノードがホームネットワークから他のエージェントが属する通信ネットワークに移って位置が変化する場合である。換言すれば、移動ノードのデータ通信ネットワークへのリンクあるいは接続があるエージェントから別のエージェントへと移る場合である。マクロモビリティはホームエージェントとフォールインエージェントとの間、あるいはフォールインエージェント間の変化であり、エージェント間モビリティとも呼ばれる。第二に、中間モビリティとは、移動ノードがそのリンクをあるBTSの属する通信ネットワークから、別のBTSの属する通信ネットワークへ移す際の、移動ノードの位置変化のことを言う。最後にマイクロモビリティとは、通信ネットワークリンクが変化せずにBTS通信ネットワーク150内の移動ノードの位置が変化する場合のことをいう。

【0032】無線移動通信ネットワークにおける中間モビリティとマイクロモビリティの取り扱い方とは良く知られている。例えば、良く知られている方法に、ピーコン信号強度を用い、移動ノード装置135がマクロモビリティスケールでその位置を変えたとき、BTS間における通信ハンドオフを行うものがある。あるいは、移動ノード135がBTS通信ネットワークの境界をまたい

で位置を変更したとき、BTS間の通信ハンドオフが行われるのも標準的な方法である。どちらの方法をとるにせよ、その詳細な説明は本発明を理解するのに特に必要ではないのでここでは省略する。

【0033】移動ノードが通信ネットワーク内において、通信ネットワークリンクをあるエージェントから別のエージェントに変更するようなマクロモビリティレベルに関して本発明が適用される。図2はモバイルIPv6を適用した、第三世代の無線移動アクセスデータ通信ネットワークにおける移動ノードのマクロモビリティとハンドオフ過程を示す簡略図である。この例において、移動ノードのマクロモビリティに起因するエージェント間の通信ネットワーク接続ハンドオフ処理は、提案されているモバイルIPv4についてはIETFのRFC2002に、提案されているIPv6については「www.ietf.org./internet-drafts」のなかの「draft-ietf-mobility-ipv6-12.txt」にそれぞれ規定されている。

【0034】図2において通信ネットワーク100はIPv6ネットワーク120およびIPv6ネットワーク120に接続されるルータすなわちエージェント145で構成される。ハンドオフ過程は移動ノード（MN）135が初めに位置Aにいるときに開始されるとする。図に示す例では、MN135はホームリンク内で動作しており、ホームエージェント145を介してネットワーク120と接続されている。MN135は、好ましくはホームエージェントHA145を含むエージェント145と無線により、CDMA、W-CDMAまたは同様な無線広帯域スペクトル拡散信号技術等を用いて、図示せぬBTSと通信を行う。

【0035】モバイルIPv6およびモバイルIPv4規格は、モビリティ検知およびハンドオフの機能を提供する。どちらのバージョンにおいても、MN135のモビリティは近隣探索（Neighbor Discovery）メカニズムによって検知され、移動ノードが最初のエージェントのカバーするエリアから2番目のエージェントがカバーするエリアへ入ったとき、最初のエージェントから2番目のエージェントへの移動ノードのネットワーク接続のハンドオフが行われることになる。従って、この例ではモバイルIPv6通信ネットワークに関して図示しているが、モバイルIPv4に関しても同様な機能および要件が存在する。

【0036】MN135が初期位置Aから中間地点である位置Bへ移動すると、その動きはIP移動検出方法または好ましい方法の組み合わせによって検出される。モバイルIPv6における主な検出方法は、IPv6のルータ発見（Router Discovery）や近隣到達不能検出（Neighbor Unreachability Detection）を含む、IPv6の近隣探索を実行する設備を用いるものである。IETFのRFC2461の「IPv6のための近隣探索（Neighbor Discovery for IP version 6）」

6)」に詳細に記載されており、本願明細書において参照のため援用される。これはIPv6の移動ノードに対し、すでに言及し本願明細書において援用されているITEFのモバイルIPバージョン6の草案において推奨されているものである。

【0037】位置Aから位置Bを経由して位置Cへと移動する間、MNはルータ発見を使って新しいエージェンツおよびリンクが張られているサブネットプレフィックスを探す。ルータ発見処理は、MNによるルータ要請メッセージのブロードキャストを含む。フォーリンエージェンツ145 (FA1) がルータ要請メッセージを受信できるくらい十分にMNの近傍にいるときは、当該フォーリンエージェンツは直接MN135に対しルータ通知メッセージを送信することになる。あるいは、MN135は単にFA1からの非請求(定期的)ルータ通知を待っているだけでも良い。MN135がFA1からルータ通知メッセージを受信すると、MNは自己のデフォルトルータリストおよび、自己のプレフィックスリスト内のFA1のサブネットプレフィックスのエントリを保持する。このようにして、デフォルトルータリストによつて、当該MN135が新しい通信ネットワーク接続を確立できるMNデフォルトエージェンツの候補のひとつとしてFA1は特定されるのである。

【0038】MN135がHA145から離れている間は、MNは、新しいエージェンツと新しい気付けアドレスとに切り替える為に、HAと送受信不可能になった時点をすばやく検知できるかどうかが重要である。デフォルトエージェンツと送受信不可能になった時点を検知するために、MN135は隣接到達検知を用いる。図2において、MN135が中間地点Bに到達し位置C方向へ移動しつつあるとき、HAを介して行われていたネットワーク接続状態は劣化する。通信状態の劣化は、MAC層(第2層)によって検出されるL2ビーコン信号強度の減少および通信エラーの増大という形で現れる。HA145から到達可能かどうかは、(1) MN135がHA145と通信しているならば、パケットに対するHA145からの応答として受信するTCP応答確認の損失があるかどうか、または(2) HA145からの非請求マルチキャストルータ通知メッセージの損失があるかどうか、または(3) 明示的隣接通知メッセージに対する応答としてHA145からの隣接通知メッセージが受信されないかどうかによって決定される。MN135がHA145との通信状態の劣化を検出し始めたら、MN135はハンドオフ処理を開始し完全にHA145と通信不能になってしまうまでの間にその処理を完了しなくてはならない。MN135はまず、デフォルトルータリストを検索しFA1を探す。次に当該FA1との通信リンクを確立し、HA145との通信リンクを切断する。

【0039】HA145とFA1との間の通信ハンドオフ処理にあたって、MN135は新たなフォーリンエ

ジェンツを特定するための気付けIPアドレスを取得する必要がある。自動アドレス設定の好ましい方法としては、ITEF RFC2462の、「IPv6 ステートレスアドレス自動設定」に規定されており、本願明細書ではこれを援用する。この方法によれば移動ノードの新たな気付けアドレスは、FA1から通知されるサブネットプレフィックスリスト内のFA1のサブネットプレフィックスから生成される。ハンドオフ処理が終了した後、MN135が位置Cに到達する時間までには、フォーリンエージェンツFA1を介してネットワークリンクが確立されることとなる。

【0040】図3は新たな気付けアドレスの登録の過程およびハンドオフ処理が完了した後の経路最適化の過程を要約した図である。ステップ1において、MN135はHA145からフォーリンエージェンツ(FA1)へとネットワーク接続のハンドオフを行う。次にMN135は、FA1から送信されるFA1のサブネットプレフィックスにより生成される気付けアドレスを設定し(ステップ2)、バインディング更新をFA1を介してHAへと送信する。HA145は当該バインディング更新を受け取ると、該気付けアドレスをMN135用のバインディングキャッシュに登録することによって、MNのホームアドレスと現在の気付けアドレスとの関連付けがなされる。バインディングキャッシュにおける関連付けにはある有効期間が設定されており、それを経過するとその関連付けは無効となる。

【0041】MN135がネットワーク接続をFA1へとハンドオフした後、相手先ノード(CN)140が該MN135と通信を開始する必要になったとする。さらに、該CN140は一度も該MN135と通信を行ったことがなく、該MNの変換することのないホームアドレスを除き、該MNの現在位置に関する情報を持っていない。従って、該CNは第一パケットを該MNのホームネットワークへ送信する(ステップ3)。HA145は、該CN140から送信されたパケットを取得し、該MNの現在の気付けアドレス用のバインディングキャッシュを検索する。次に、HA145はこのパケットをカプセル化したのち、新たなパケットを生成し、これを該FA1を介して現在のMNの気付けアドレスをあて先として該MN135へトンネル送信する。

【0042】「HYPERLINK "http://www.ietf.org/internet-drafts" www.ietf.org/internet-drafts」に掲載されている「draft-ietf-mobileip-optim-09.txt」において規定されている、提案中の拡張モバイルIPv4規格では、MN135とCN140との間で直接通信経路を確立することによって、パケットルーティングの最適化が図られている。この提案中の拡張規格の本質的な部分は、既述したようにモバイルIPv6規格にすでに組み込まれている。MN135は、HA145からカプセル化されトンネル送信されたパケットを受信すると、該

Hアルゴリズムを置き換えるものである。ケルベロスは他のセキュリティ保護がされていないネットワークに対し、既共有秘密鍵に基づいて秘密鍵暗号化アルゴリズムを用いた認証サービスを提供する。I T E F 1 5 1 0 の「ケルベロスネットワーク認証サービス (The Kerberos Network Authentication Service (V5))」に詳細な記載があり、これを本明細書において参照のため援用することとする。

【0049】前述した規格で提案される I P s e c は、その実行および鍵管理の対応する準備ができていながらも、ケルベロスを用いる事に関しては何も言及していない。実際、ケルベロス等の方法は当該提案されている I P s e c の枠組みにはうまく適合しない。R F C 2 4 0 1 において定義されている、I P s e c の集中鍵管理を作成するための標準化過程プロトコルを取り決めるために結成されたワーキンググループは、現在、R F C 1 5 1 0 で定義されているケルベロスアーキテクチャを用いて I P s e c 用の暗号化音声プロトコル作成中である。

【0050】ケルベロスは従来の暗号化技術すなわち、信頼できる第3者の認証サービス機関から配布される共有秘密鍵を用いて認証を行う。図4は、ケルベロス鍵交換方法を用いたユーザ認証確立までの処理と S A の設定とを簡単にまとめた図である。ノード a およびノード b は信頼できる第3者認証サービス機関である同一の鍵配布センタ (K D C) の管轄であり、各ノードはそれぞれ既登録の秘密鍵 K a および K b を K D C に保有している。たとえば、ノード a とノード b とがある一つのネットワークに接続しているとき、これらの秘密鍵は K D C に登録される。したがって、ノード a と K D C は秘密鍵 K a を共有し、ノード b と K D C は秘密鍵 K b を共有していることになる。秘密鍵 K a および K b は通常半永久的に変わらないものと考えてよい。

【0051】ここで、ノード a がノード b と通信を行うにあたって、K D C に対して、ノード a とノード b 間の通信の暗号化・復号化に必要なセッション鍵の発行を依頼するとする (ステップ1)。この依頼に対し、K D C はセッション鍵 S a b を準備するとともに、秘密鍵 K b を用いてセッション鍵 S a b を暗号化した鍵を準備する。このセッション鍵 S a b は、特にノード a とノード b 間での通信のセッションを暗号化・復号化するのに用いられ、従って秘密鍵 K a および K b とは異なり、短い有効期間しか持たない。次に K D C は秘密鍵 K a を用いて、セッション鍵 S a b および秘密鍵 K b で暗号化されたセッション鍵 S a b の両方を暗号化しノード a へ送信する (ステップ2)。ノード a は復秘密鍵 K a を用いて、受け取ったセッション鍵 S a b と、秘密鍵 K b で暗号化されたセッション鍵 S a b (第2の鍵) とを復元する。第二の鍵は秘密鍵 K b によって暗号化されているため、ノード a はこれ以上この鍵を復号化することができ

ない。ステップ3ではノード a はこの第二の鍵をノード b へ送信する。ノード b は秘密鍵 K b を用いてこの第二の鍵を復号化しセッション鍵 S a b を復元する。このようにノード a およびノード b はセッション鍵 S a b を共有することで、当該ノード間における以降の通信において、通信の暗号化および復号化がなされる。ノード b が秘密鍵 K b を用いて第二の鍵を復号化できるということは第二の鍵が K D C で発行されたものであるということである。なぜなら、K D C とノード b だけが秘密鍵 K b を知っているからである。また、各ノード a および b は以降の通信をセッション鍵 S a b を用いて復号化することができるということは、送信者の認証ができるということでもある。なぜなら、K D C、ノード a、ノード b だけがセッション鍵 S a b を知っているからである。

【0052】図5から図7を用いて本発明の好適な方法の詳細を説明する。図5から図7は本発明の I P s e c を実行する方法を示したフローチャートである。これらの図におけるデータ通信ネットワークは図3におけるものと同一である。すなわち、第三世代若しくはそれを超える世代の無線移動アクセスインターネットプロトコルベースのデータ通信ネットワークあるいは無線 LAN である。したがって、図中のネットワークは I、P v 4 規格と I P v 6 規格とに適合し、モバイル I P v 4 および I P v 6 の両方をサポートする。当該ネットワークは I M T - 2 0 0 0 規格にも適合し、C D M A、W - C D M A またはその他の無線広帯域スペクトル拡散信号処理技術を用いた無線による移動アクセスをサポートする。図に示す態様においては、V o I P によるリアルタイム双方向マルチメディアデータ通信がネットワーク内で行われる。また、図に示されている処理は M N 1 3 5 が H A 1 4 5 からハンドオフを完了し、当該 M N の気付けアドレスが H A 1 4 5 に登録されたときに始まるものである。さらに、図中の K D C は二つのサーバとしての機能を有する。すなわち、認証サーバ (A S) とチケット交付サーバ (T G S) である。A S は T G S に対するノードの認証を行う。T G S は、お互いに通信を望んでいるノードに対しセッション鍵およびチケットの発行を行う。

【0053】図5において相手先ノード (C N) 1 4 0 は M N と通信を開始しようとしている。C N 1 4 0 のバインディングキャッシュは当該 M N の現在の気付けアドレスはまだ更新されていないとする。C N は当該 M N と通信を行うために、まず C N は当該 M N に対して第一パケットを当該 M N のホームネットワークへ送信する (ステップ1)。第一パケットは制御パケットであり、その中身は実行すべきアプリケーションによるが、一例を挙げれば、V o I P における単なる接続要求である。第一パケットは常に保護すべきデータを含んでいるとは限らないので、I P s e c の保護なしで送信されてもかまわないと考えられる。この第一パケットは H A によって受

MNのホームアドレスと該MNの現在の気付けアドレスが関連付けているバインディング情報を該CN140が持っていないことを認識する。ステップ4において、該MN135はバインディング更新を該CN140に送信する。該CN140はバインディング更新を受信すると、バインディングキャッシュに該MNの恒久的なホームアドレスと関連づけて格納されている該MNの気付けアドレスのエントリを保持する。この後、該CN140から送信される該MN135宛の全てのパケットは、該CN140から該MN135へ直接伝送される。従って、このような経路最適化をおこなうことにより、いわゆるトライアングル・ルーティングに起因するパケット遅延の問題は解消される。

【0043】上述したバインディング処理において、該MN135の正当性を担保するため、および盗聴、能動的リプレイ攻撃、その他の攻撃、秘密データへの不正アクセス等の問題を回避するため、該MN135と該CN140間において、認証およびセキュリティアソシエーションも行われる。特に、もしバインディング更新を送信しているMN135がCN140において正しく認証されていない場合、あるいは、以降の通信に必要な正しいセキュリティアソシエーションがMN135とCN140間で確立されていない場合、この経路最適化機能は深刻なセキュリティ上の問題を引き起こす可能性がある。本願明細書においてすでに援用されているIETFのモバイルIPv6の草案にはこれらのセキュリティ上の問題が指摘されている。

【0044】IETFのRFC2401の「Security Architecture for the Internet Protocol」(本願明細書においてすでに援用済み)において、IPv4およびIPv6の両方について、暗号ベースのIPセキュリティ(IPsec)の基本的なアーキテクチャが提案されている。IPsecは認証および秘匿性(暗号化)を含むセキュリティ上のサービス群を提供する。RFC2401にしたがえば、IPsecはふたつのセキュリティプロトコル、すなわち認証ヘッダ(AH)と暗号ペイロード(ESP)、および暗号鍵管理の手続きおよびプロトコルを用いて実行される。AHとESPはIPsecを実行する上において重要な役割をする。その詳細はRFC2402の「IP Authentication Header」およびRFC2406の「IP Encapsulating Security Payload」に記載されており、参照のため本願明細書において援用する。暗号鍵管理手続きおよびプロトコルについては、RFC2408の「Internet Security Association and Key Management Protocol (ISAKMP)」に記載があり、これは本願明細書にすでに援用済みである。

【0045】RFC2401で提案されているセキュリティ方式およびプロトコルのなかで、セキュリティアソシエーション(SA)はIPsecの実行の際に最も基本となるものである。SAは二つのノード間の関係であ

り、お互いのノードが安全に通信を行うことを目的として、使用することを合意しているセキュリティサービスを記述するものである。SAはセキュリティパラメータインデックス(SPI)とIP送り先アドレスとセキュリティプロトコル(AHまたはESP)識別子との3つによって一意に決定される。SPIはセキュリティプロトコルの識別子である。IP送り先アドレスは、通信相手ノードのホームアドレスまたは気付けアドレスを示している。各々のノードは、現在通信中のノードまたはすでに通信したことのあるノードの各々に対し、一つのSAを持っている。各SAには予め決められた時間が経過すると無効になるような有効期間が設定されている。ノード間で保護されるべきデータを含んだパケットがやり取りされる前にSAが設定されなければならない。

【0046】SAの設定は、RFC2401で提案されているような暗号ベースのIPsecにおける鍵管理プロトコルの重要な部分である。暗号ベースのIPsecの背景にある基本的な考え方は、通信の暗号化および復合化の際に使われる秘密セッション鍵を二つのノードが共有するという点にある。よって、SAを設定するには必ず秘密セッション鍵の設定が必要になる。鍵の設定には二つの方法がある。一つは鍵輸送とよばれ、信頼できる第三者機関である鍵配布センタ(KDC)が、ネットワークドメイン内にある全てのノードの秘密セッション鍵を保有し、通信を開始したいノードに対して秘密セッション鍵を配布するというものである。もう一つは鍵生成と呼ばれる方法である。この鍵生成の例として、秘密セッション鍵を生成するためにディフィ・ヘルマン(Diffie-Hellman; D-H)アルゴリズムを用いるものがある。D-Hアルゴリズムは二人のユーザが公開鍵を交換することから始まる。各ユーザは他のユーザの情報を自分の情報とを数学的に結合させ秘密の値を算出するのである。この秘密の値は、セッション鍵としてまたはランダムに生成されるセッション鍵を暗号化する場合に必要となる鍵として用いられる。

【0047】ユーザ認証およびSAの設定を実行するのにかなり時間がかかり、パケット遅延をもたらすことは当業者にとって明らかである。本発明はユーザ認証およびSAの設定によるパケット遅延の問題の解決を図ることを目的としている。本発明は、相手先ノードは、移動ノードが第一パケットを相手先ノードから受信した後ユーザ認証およびSAセキュリティの設定を初期化するのを待つのではなく、自ら初期化処理を実行することができるとする方法を提供する。

【0048】さらに、本発明は、移動ノードと相手先ノード間で伝送されるデータの暗号化・復号化を行う際に一般的に用いられているが多大な量の計算を必要とするため深刻なパケット遅延を招きかねない従来のD-H公開鍵アルゴリズムに取って代わるものである。本発明は、比較的計算の負荷が少ないケルベロス鍵交換方法でD-

信されHAから当該MNへトンネル送信される(ステップ2)。CNで実行すべきアプリケーションにも依存するが、この第一パケットは制御パケットでなくとも良く、当該MNに送信される前にIPsecによって保護されたデータであっても良い。そのような場合、ステップ1および2は省略され、すぐにステップ3に移り、当該CNと当該MN間でセキュリティアソシエーション(SA)が設定される。

【0054】図5におけるネットワークの全ての構成要素は、IPsecを実行するための第一の手段としてケルベロスを用いることに同意している。従って、ネットワークは一つの鍵配布センタ(KDC)を備え、ここで当該ネットワークで用いられる全ての暗号鍵を管理している。上述したようにKDCは認証サーバ(AS)およびチケット交付サーバ(TGS)で構成される。さらに、MNとKDCは、当該MNが当該ネットワークにログインした時点で発行された秘密鍵 K_{mn} を共有している。CNおよびKDCは同様にCNがネットワークにログインした時点で発行された秘密鍵 K_{cn} を共有している。購入時に秘密鍵を作り、KDCと秘密鍵を共有し、ネットワークにアクセスするための機器にはいろいろな種類がある。

【0055】第一パケット送出した後、CNはセキュリティアソシエーション(SA)キャッシュを参照し、当該MNとの間で設定済みのSAがあるかどうかをチェックする(ステップ3)。図8は本実施形態で用いられるSAキャッシュを示す。図において、SAキャッシュには複数のSAエントリがある。ひとつのSAエントリは、当該CNが現在通信しているかまたは過去に通信したことがあるひとつのノードに対応している。SAは、セキュリティパラメータインデックス、セキュリティプロトコル識別子およびIP送信先アドレスを含むいくつかのパラメータによって特定される。この3つのパラメータについてはすでに説明したのでここでは省略する。この3つのパラメータに加えて、本実施形態におけるSAはさらに二つのパラメータを有する。一つは「IP送信先ホームアドレス」と呼ばれるもので、もうひとつは「第一パケットフラグ」と呼ばれるものである。IP送信先ホームアドレスには、通信相手のノードのホームアドレスが格納されている。第一パケットフラグは、第一パケットが、SAが設定されていない状態でノードに送信されたときにオンとなり、他方SAが設定されたときオフとなる。SAには有効期間があり、ある時間が経過すると無効になる。すなわち、有効期間が経過するとSAエントリは当該SAキャッシュから消去される。

【0056】図5ステップ3において、CNは自身のSAキャッシュを検索し、当該MNに対するSAエントリがあるかどうかを確かめる。MNに対するSAキャッシュがある場合、CNはステップ4の処理に進み以降のパケットは、SAキャッシュに格納されているセキュリティ

イパラメータインデックスによって特定されるケルベロスセッション鍵を用いて暗号化され、当該MNへ送信される。該当するSAエントリが存在しない場合、CNはステップ5の処理に進む。CNが当該MNと一度も通信を行ったことがない場合、当該MNに対するSAエントリは存在しない。

【0057】さらに、CNがMNと以前通信を行ったことはあるが、それがかなり昔である場合、当該MNに対するSAエントリは無効になっており、SAキャッシュからも消去されている。当該MNに対するSAエントリが見つからなかった場合、以降のMNとの通信を保護するために、新たなSAを設定する必要がある。従来のIPsecプロトコルにおいては、このような場合、バインディング更新をMNから受信した時点でCNはSAの設定を開始していた。具体的には、MNがCNからの送信されHAによってトンネル送信された第一パケットを受信すると、該MNはCNが現在のMNの位置を知らないということを認識し、当該CNに対してバインディング更新を送信し、当該CNは自身のバインディングキャッシュを更新するのである。CNがMNから送信されたバインディング更新を受信した後、SAが設定される。換言すれば、従来のIPsecにおいては、MNはCNへバインディング更新を送信することによってSAを初期化するのである。しかしながら、SAがMNとCNとの間で設定されるまで、実質的に両者の間で通信を行うことはできない。よって、従来のIPsecを用いたSAの設定においてはバインディング更新がCNに届くまでSAの設定を開始することができないために重大なパケット遅延をもたらすということは当業者にとって容易に分かることである。

【0058】本発明においては、CNは、MNがCNからの第一パケットを受信した後SA設定の初期化するので待つのではなく、CNがSA設定の初期化を行うことができる。ステップ5においてCNは、図8に示す自身のSAキャッシュ内に当該MNに対するSAエントリを1つ指定し第一パケットフラグをオンにする。第一パケットフラグがオンであるということは、すなわちSAの設定が現在行われているということ意味する。セキュリティ保護されるべきパケットデータはSAが設定されるまで送信することができないが、制御パケットは保護されていない状態で送信することができる。

【0059】CNは以降の制御パケットをMNに対して送信することは許されるが、第一パケットフラグによって、MNとの間でのSAの設定を繰り返し初期化することは禁止される。次に、CNはKDCと通信を行うことが許可されているかどうかを判断する。具体的には、CNは自身をKDCに認証してもらうためのケルベロスチケットを自身が持っているかどうかを判断する。持っていない場合、最初の認証処理(ステップ6)へ進み、KDCからチケットを取得する。すでに持っていた場合

は、ステップ7へと進み、KDCに対して、当該MNと通信を行えるようにするため、認証サービスを要求する。

【0060】ステップ6の詳細を図6に示す。最初の認証ステップ（ステップ6）において、ユーザはまずユーザ名を入力するよう求められる（ステップ6-1）。続いて、CNはケルベロス認証要求（KRB_AS_REQ）を該ユーザ名とともにASへ送信する（ステップ6-2）。ユーザ名の確認および秘密鍵K_{cn}の抽出後、ASはセッション鍵S_{cn}およびチケットT_{cn}を生成する（ステップ6-3）。ASはセッション鍵S_{cn}およびチケットT_{cn}を、秘密鍵K_{cn}を用いて暗号化したうえで、これをケルベロス認証応答（KRB_AS_REP）としてCNへ送信する。K_{cn}（S_{cn}、T_{cn}）はセッション鍵とチケットT_{cn}との両方が秘密鍵K_{cn}で暗号化されたことを意味する。CNはKRB_AS_REPを受信すると、秘密鍵K_{cn}で復号化しセッション鍵S_{cn}およびチケットT_{cn}を復元する（ステップ6-5）。CNは自身をTGSに対して認証してもらうためのチケットT_{cn}を取得したので、ステップ7へ進む。ステップ7の詳細を図7に示す。

【0061】図7においてCNはTGSに対し、チケットT_{cn}とともに、MNと通信するためのセッション鍵の発行を要求を送信する（ステップ7-1）。チケットT_{cn}はTGSに自身を認証させるための証明書役割を持つ。チケットT_{cn}の認証が完了した後（ステップ7-2）KDCはステップ3においてセッション鍵S_{cn}/mn、セッション鍵S_{mn}およびチケットT_{mn}を生成する。セッション鍵S_{mn}はMNとKDC間の通信を保護するために利用され、チケットT_{mn}はMNをKDCに認証させるための証明書として用いられる。MNはKDCと通信を行い、セッション鍵S_{mn}およびチケットT_{mn}がすでに設定されている場合、TGSはこの鍵およびチケットを発行することはない。

【0062】まず、セッション鍵S_{cn}/mn、セッション鍵S_{mn}およびチケットT_{mn}が秘密鍵K_{mn}を用いて暗号化される（K_{mn} {S_{cn}/mn, T_{mn}, S_{mn}}）。次にTGSはセッション鍵S_{cn}/mnとK_{mn} {S_{cn}/mn, T_{mn}, S_{mn}}の両方を秘密鍵K_{cn}を用いて暗号化（K_{cn} {S_{cn}/mn, K_{mn} {S_{cn}/mn, T_{mn}, S_{mn}}）し、CNへ送信する（ステップ7-4）。ステップ7-5においてCNは秘密鍵K_{cn}を用いてこれらの鍵を復号化しセッション鍵S_{cn}/mnおよびK_{mn} {S_{cn}/mn, T_{mn}, S_{mn}}を取り出す。K_{mn} {S_{cn}/mn, T_{mn}, S_{mn}}は秘密鍵K_{mn}によって暗号化されているのでCNはこれ以上復号化することはできない。次にCNはK_{mn} {S_{cn}/mn, T_{mn}, S_{mn}}を送信するがこれらはHAによって受信され、MNへトンネル送信される（ステップ7-6）。MNはK_{mn} {S_{cn}/

mn, T_{mn}, S_{mn}}を受信するとこれを秘密鍵K_{mn}を用いて復号化しセッション鍵S_{cn}/mn、T_{mn}、S_{mn}を取り出す（ステップ7-7）。

【0063】図5に戻りステップ7の処理が完了すると、CNは自身のSAキャッシュに格納されている、当該MNと通信を行うために設定されたSAのエントリを保持する（ステップ8）。具体的には図8に示すSAキャッシュにおいて、CNは、セッション鍵S_{cn}/mnを特定するためのセキュリティパラメータインデックスを含む必要な情報を当該MNに対するSAエントリに格納する。CNはさらに、同一のエントリの第一パケットフラグをオフにする。対応するSAエントリはMNのSAキャッシュ内にも生成される。

【0064】CNおよびMNは同一のセッション鍵S_{cn}/mnを共有するので以後安全に通信を行うことができる。最後に、MNは、CNから送信された第一パケットの応答として、バインディング更新をCNに送信する（ステップ9）。本発明の方法を用いれば、CNがSA設定を初期化することができるのでSA設定に起因するパケット遅延が劇的に減少する。

【0065】図9は本発明の別の実施形態を示したものである。本実施形態において、上記のCNが移動ノードの場合、移動ノードと無線通信ネットワーク制御装置（RNC）との間における第二層における認証用の秘密鍵が第三層における認証用の鍵としても用いられる。RNCは呼制御、接続制御、無線インターフェースサポートおよびモビリティ管理のような第二層通信プロトコルを実装している。移動ノードがネットワークに対して初めて無線接続を試みると、RNCに対して当該移動ノードを認証させるための第二層の秘密鍵が生成される。

【0066】他方、上記秘密鍵K_{mn}およびK_{cn}はKDCとの間で生成され、第三層での認証の際に使用される。換言すれば、移動ノードからネットワークに対し無線による接続が確立されたとき、当該移動ノードは第二層での認証用の秘密鍵を持っていなければならない。接続が確立した後、当該移動ノードは自身をKDCに認証させるために、別の、第三層における認証用の秘密鍵を持っている必要がある。確かに二つの鍵の使用目的は異なるが、二つの別途独立した秘密鍵を生成することは煩雑でかつ無駄であるということは当業者にとって明らかである。従って、本実施形態においては、このような無駄を省くため第二層の秘密鍵が第三層の秘密鍵としても利用できるようになっている。

【0067】図9に一つの秘密鍵が第二層と第三層の両方の認証に対して用いられる無線データ通信ネットワークを示す。同図においてCNは移動ノードであり、無線接続が確立したとき、自身とRNCとの間の通信で用いる第二層の秘密鍵を生成する（ステップ1）。第二層の秘密鍵がRNCから当該通信ネットワーク上にあるKDCに送信される。CNの内部では、第二層の秘密鍵は第

三層へ通知される。従ってCNおよびKDCは同一の秘密鍵を共有することとなる。CNをKDCに認証させるために、CNとKDC間における第三層の秘密鍵を生成する必要はない。CNがMNと通信をする必要がある場合には、CNは上述したように、SA設定を初期化しKDCに対して、CNと当該MN間で通信を行うためのセッション鍵の発行を要求する(ステップ3)。

【0068】CNはセッション鍵の発行要求を受信すると、KDCと共有している当該CNの第二層の秘密鍵を用いて、自身をKDCに認証させる。次にKDCは、セッション鍵およびMNの第二層の秘密鍵で暗号化したセッション鍵をCNへ送信する。ついで、この二つの鍵は自身の秘密鍵によって復号化される(ステップ4)。次に当該CNは、まだMNの第二層の秘密鍵によって暗号化されている当該セッション鍵をMNへ送信し(ステップ5)、MNの秘密鍵によってこのセッション鍵は復号化される。

【0069】図10は本発明の更に別の態様を示したものである。セッション鍵は通信のセッションを保護するために発行され、ある有効期限を持つ。したがって、新たな通信セッションが始まる時は新たなセッション鍵をKDCから取得しなければならない。また、予期せぬ通信上の問題のため、通信セッションが完了するのに時間がかかってしまう場合、セッション鍵はセッションの途中で無効になってしまう可能性もある。

【0070】仮にセッション鍵がセッションの途中で無効になったとすると、当該通信セッションは中止せざるを得ず、新たなセッション鍵をKDCから取得するまでは通信を再開することができない。図10に示すネットワークにおいて、セッション鍵の有効期間は長く、複数の通信セッションに渡って再使用すること可能である。しかしながら、セッション鍵の有効期間を長くするとノードは多くのSAエントリを持っていなければならない可能性がある。通常、移動ノードは、多くのSAエントリを格納しておくだけの十分なメモリ空間を有していない。この問題を解決するために、図10におけるネットワークは、当該ネットワークに接続される移動ノードに代わってSAを管理するSA管理装置を備えている。

【0071】図10において、CNがMNと通信を行う必要が生じたとき、当該CNは上述したようにSA設定を初期化しセッション鍵の発行を自己のSA管理装置Aに要求する(ステップ1)。当該SA管理装置Aは、この要求に対する応答として、当該CNと当該MN間の通信を保護するためのSAの設定に対するSAエントリを検索する。SAの有効期間は長いので、当該CNと当該MNと以前に通信を行ったことがある場合、CNとMNとの間での以前に行われた通信に対して設定されたSAがまだ残っている可能性がある。

【0072】SA管理装置Aがまだ以前の通信に対する

SAを保存している場合、当該SA管理装置はSAによって特定されるセッション鍵を当該CNへ送信する。ついで当該CNは、以前に当該MNと通信で使われたこのセッション鍵で暗号化したパケットを当該MNへ送信する。当該MNは当該CNよりこのパケットを受信すると、自己のSA管理装置Bに対してCNから受信したパケットを復号化するためのセッション鍵の発行を要求する。セッション鍵の以前の通信からの有効期間は、SA管理装置Aと(B)で同一である。従って、同一のセッションはSA管理装置Bでもいまだ有効であるはずである。SA管理装置Bは要求の応答として、セッション鍵を当該MNへ送信する。当該MNはSA管理装置Bから受け取ったセッション鍵を用いてCNから受信したパケットを復号化する。

【0073】SA管理装置AがCNとMNの間の通信に関するSAを持っていない場合は、SA管理装置AはKDCに対し、新たなセッション鍵の発行を要求する(ステップ2)。これに対しKDCはセッション鍵を当該SA管理装置Aへ送信する(ステップ3)。SA管理装置AはMNとの通信を行うためのSAを内部で生成し、当該セッション鍵をCNとSA管理装置Bへと送信する(ステップ4)。次に、SA管理装置Bは対応するSAを設定し、当該セッション鍵MNへ送信する(ステップ5)。

【0074】上述したように、当該セッション鍵は、CNの秘密鍵とMNの秘密鍵とによって保護された状態で、KDCとCN間およびCNとMN間で配布される。SAの有効期限は長い(したがってセッション鍵のそれも長くなる)ため、KDCに鍵の発行を要求する頻度は少なくてすむ。しかるに、KDCがセッション鍵を発行することに起因するパケット遅延も減少する。また、伝送されるパケットの数に基づいて通信コストは算出される。KDCに対するセッション鍵の発行要求の回数が少なくなるので、SAを設定するために必要なパケットの数も減少し、通信コストの削減になる。

【0075】図11は本発明の更に別の実施形態を適用した無線データ通信ネットワークを示す図である。図10に示した実施形態と同様、SAおよびセッション鍵の有効期間は長い。しかしながら、図11に示す本実施形態においては、SAは携帯電話内の購入者識別モジュール(SIM)に格納される。SIMはマイクロチップが組み込まれたスマートカードである。

【0076】マイクロチップには、購入者のアカウントの詳細がサービスへのアクセス情報および設定情報とともに格納されている。本実施形態で導入されるIPsecプロトコルは図10に示す実施形態のそれと同様である。すなわち、CNはMNと通信を行う必要になったとき、当該CNは携帯電話PcnのSIMに格納された、当該CNと当該MN間での通信を保護するために設定されたSAのSAエントリを参照する。

【0077】携帯電話機PcnのSIMが以前の通信で設定されたSAをまだ保有している場合は、当該SIMはそのSAで特定されるセッション鍵をCNに通知する。CNは以前に行われた通信で用いられたセッション鍵を用いて暗号化されたパケットをMNへ送信する。MNはCNから暗号化されたパケットを受信すると、携帯電話機PmnのSIMに格納されたセッション鍵を取得し、当該携帯電話機PmnのSIMから取得したセッション鍵を用いて、CNから受信したパケットを復号化する。

【0078】CNとMN間での通信のSAが携帯電話機PcnのSIMに格納されていない場合は、CNはKDCに対して新しいセッション鍵の発行を要求する(ステップ1)。これを受けてKDCは当該CNにセッション鍵を送信する(ステップ2)。CNはMNとの通信用のSAを生成し、携帯電話機PcnのSIMに格納する。次にCNはこのセッション鍵をMNへ送信する(ステップ3)。そしてMNは対応するSAを生成し、携帯電話機PmnのSIMに格納する。

【0079】上述したように、セッション鍵はCNの秘密鍵とMNの秘密鍵とによって保護された状態で、KDCとCN間およびCNとMN間での配布される。図10に示す実施形態と同様に、本実施形態においても、SAおよびセッション鍵の有効期間が長いので、KDCに対してセッション鍵の発行の要求頻度は少ない。したがって、KDCのセッション鍵の発行に起因するパケット遅延は減少する。KDCに対してセッション鍵の発行要求の頻度が少ないということはSAを設定するために必要なパケット数も少なく済み、通信コストの削減になるということである。加えて、本実施形態においては、図10に示されるような、通信に介在するSA管理サーバ等の中間サーバは必要ではないので、通信の安全性は増す。

【0080】ここまで本発明の好適な実施形態について説明してきたが、各実施形態は単なる例示であり本発明の本質を限定するものではない。また、本発明の趣旨を逸脱しない範囲において、本発明の新規および優位な特徴を保ったままで、本発明に対し種々の変形あるいは付加を施すことは、当業者にとって容易に理解される。したがって、本発明の範囲は正しく解釈された請求の範囲のみに基づいて定まるものである。

【0081】

【発明の効果】以上説明したように、本発明の方法によれば、必要な認証およびセキュリティアソシエーション設定過程で生ずるパケット遅延が減少する。

【図面の簡単な説明】

【図1】 本発明が実施される第三世代の無線モバイルアクセスIP通信ネットワークの模式図である。

【図2】 モバイルIPを用いた第三世代の無線モバイルアクセスIP通信ネットワークにおけるモバイルノードを示すマクロモビリティを示す簡略図である。

10 【図3】 モバイルIPを用いた第三世代の無線モバイルアクセスIP通信ネットワークにおけるモバイルモビリティと経路最適化の結果を示す簡略図である。

【図4】 ケルベロス鍵交換方法の実行ステップを示す簡略図である。

【図5】 本発明のIPsecを実行過程を示すフローチャートである。

【図6】 本発明における最初の認証過程と鍵発行過程とを示すフローチャートである。

20 【図7】 本発明における共有鍵の設定の過程を示すフローチャートである。

【図8】 本発明において用いられるセキュリティアソシエーションの模式図である。

【図9】 レイヤ2の秘密鍵がレイヤ3の秘密鍵としても用いられる、本発明の第2実施形態を実行するモバイルIP通信ネットワークの簡略図である。

【図10】 ノードのセキュリティアソシエーションを管理するセキュリティアソシエーション管理装置を用いた、本発明の第三実施形態を実行するモバイルIP通信ネットワークの簡略図である。

30 【図11】 セキュリティアソシエーションが携帯電話機の加入者識別モジュール格納される、本発明の第4実施形態を実行するモバイルIP通信ネットワークの簡略図である。

【符号の説明】

100 移動IPネットワーク

FA フォーリンエージェント

HA ホームエージェント

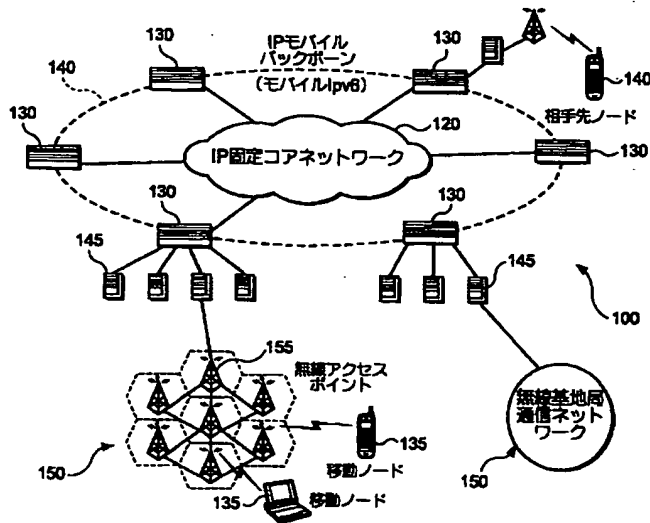
MN 移動ノード

CN 相手先ノード

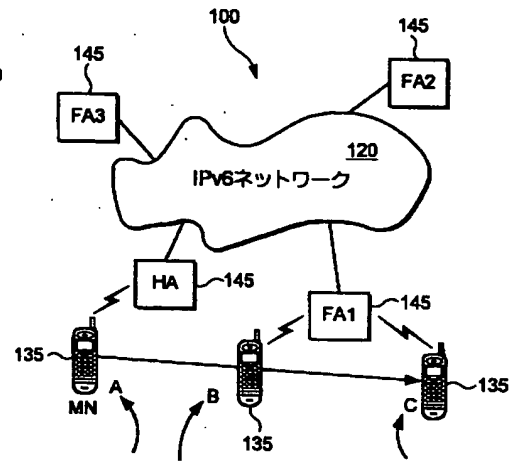
40 KDC 鍵配布センタ

RNC 無線通信ネットワーク制御装置

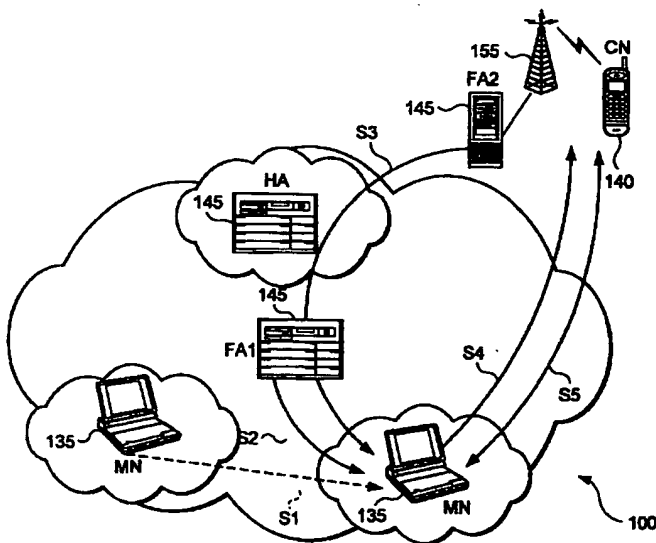
【図1】



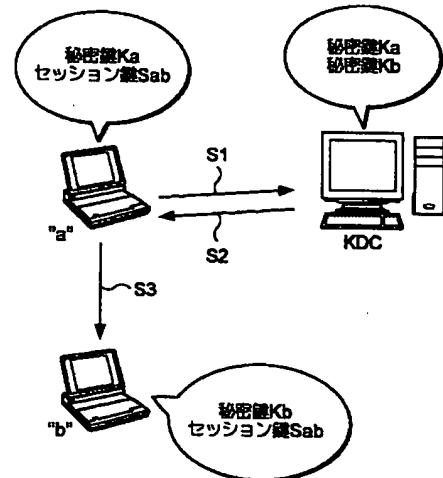
【図2】



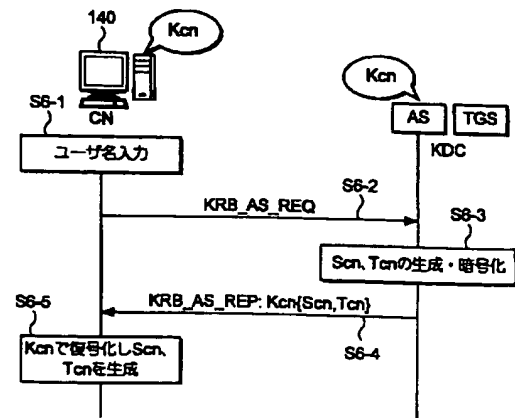
【図3】



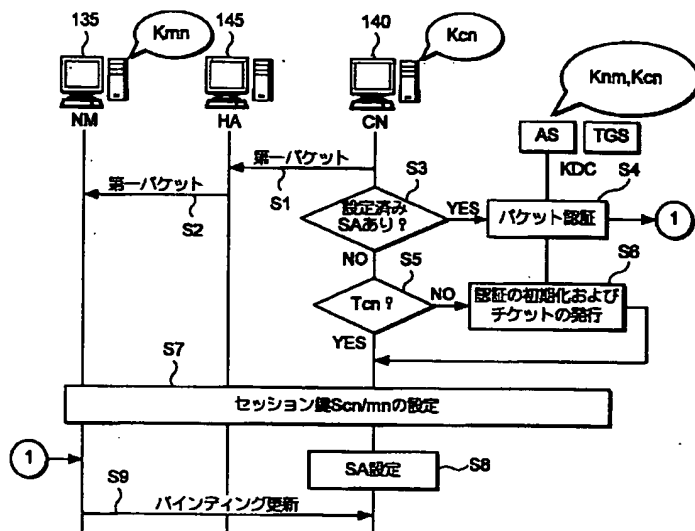
【図4】



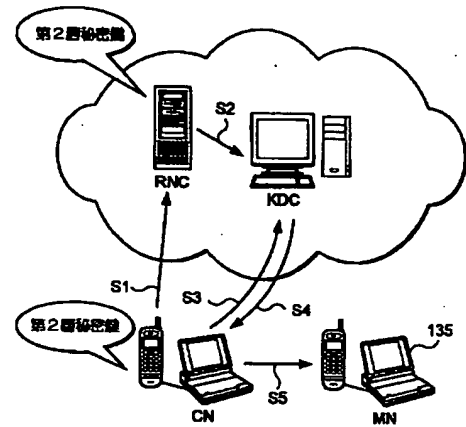
【図6】



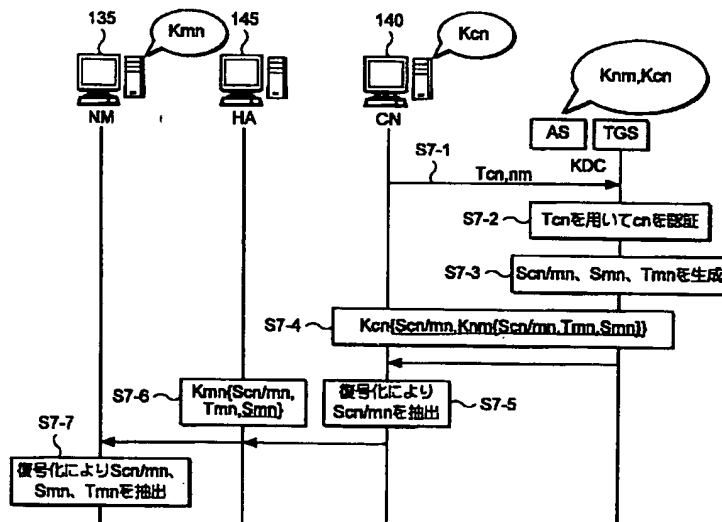
【図5】



【図9】



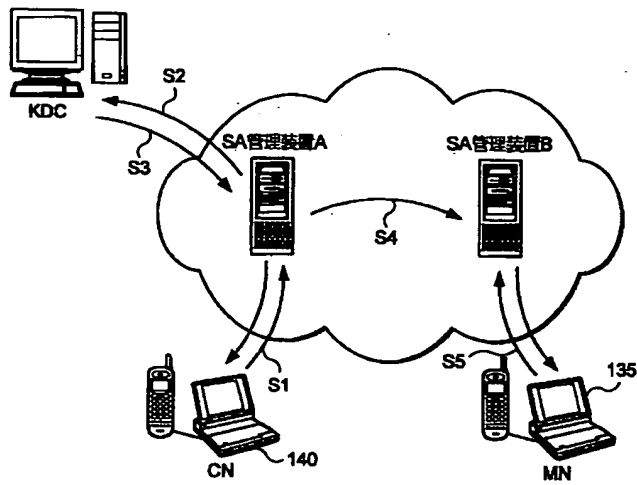
【図7】



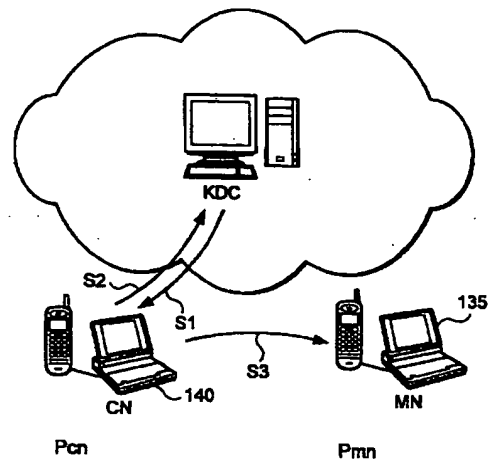
【図8】

セキュリティ パラメータ インデックス	セキュリティ プロトコル 識別子	IP送り先 アドレス	...	IP送り先 ホームアドレス	第一パケット フラグ

【図10】



【図11】



フロントページの続き

(72)発明者 ヨコテ アキ
アメリカ合衆国, カリフォルニア州
95110, サンノゼ, スイート300, メトロ
ドライブ181

Fターム(参考) 5J104 PA07
5K030 GA15 HA08 HC09 JT09 LD19
5K067 AA30 AA32 BB21 DD17 EE02
EE10 EE16 HH21 HH36

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.